CMD - Windows commands

The equivalent to the Linux command `;` as in

```
echo "command 1" ; echo "command 2"
```

is

```
dir & whoami
```

Dealing with files and stuff

Delete file

```
del
```

Create folder/directory

```
md folderName
```

Show hidden files

```
dir /A
```

Print out file content, like cat

```
type file.txt
```

grep files

```
findstr file.txt
```

Network

Show network information

`netstat -an`

Show network adapter info

`ipconfig`

Ping another machine

`ping 192.168.1.101`

Traceroute

`tracert`

Processes

List processes

`tasklist`

Kill a process

`taskkill /PID 1532 /F`

Users

```
net users

:: Add user
net user hacker my_password /add
net localgroup Administrator hacker /add

:: Check if you are part of a domain
net localgroup /domain

:: List all users in a domain
net users /domain
```

Other

Shutdown

```
:: Shutdown now
shutdown /s /t 0

:: Restart
shutdown /r /t 0
```

cipher - Clear data/shred

```
:: Shreds the whole machine
cipher /w:C:\
```

Show environmental variables

```
set
```

Show options for commands

The "man"-pages in windows is simply:

```
help dir
```

Mounting - Mapping

In the windows world mounting is called mapping.

If you want to see which drives are mapped/mounted to your file-system you can use any of these commands:

```
::This is the most thorough

wmic logicaldisk get deviceid, volumename, description

::But this works too
wmic logicaldisk get name
wmic logicaldisk get caption

::This can be slow. So don't kill your shell!
fsutil fsinfo drives

::With powershell
get-psdrive -psprovider filesystem

::This works too, but it is interacive. So it might be dangerous work hackers
diskpart
list volume

::Map only network drives
net use
```

The command to deal with mounting/mapping is **net use**

Using `net use` we can connect to other shared folder, on other systems. Many windows machines have a default-share called IPC (Interprocess communication share). It does not contain any files. But we can usually connect to it without authentication. This is called a **null-session**. Although the share does not contain any files it contains a lot of data that is useful for enumeration. The Linux-equivalent of `net use` is usually `smbclient`.

```
net use \\IP address\IPC$ "" /u:""
net use \\192.168.1.101\IPC$ "" /u:""
```

If you want to map a drive from another network to your filesystem you can do that like this:

```
:: This will map it to drive z
net use z: \\192.168.1.101\SYSVOL

:: This will map it to the first available drive-letter
net use * \\192.168.1.101\SYSVOL
```

Here you map the drive to the letter `z`. If the command is successful you should now be able to access those files by entering the `z` drive.

You enter the z-drive by doing this:

```
C:\>z:
Z:\

:: Now we switch back to c
Z:\>c:
C:\
```

** Remove a network drive - umount it**

First leave the drive if you are in it:

```
c:
net use z: /del
```

References and Stuff

This might come in handy for the linux-users: http://www.lemoda.net/windows/windows2unix/windows2unix.html